Procedure For Updating DHCP Relay To Be R80.10 Upgrade Ready

Bryce Schumacher
Security Engineer – Enterprise Accounts
Created On: April 26th, 2018
Last Updated: September 9th, 2018

Procedure Summary

This document will cover the procedure on how to move from using legacy IPv4 BOOTP/DHCP objects used in R77.30 and previous Check Point versions to new IPv4 BOOTP/DHCP objects that are used in R77.20 and future versions. This is a warning that does come up in the R80.10 pre-upgrade verification, and the exact warning is:

Legacy DHCP Relay Services - Change in behavior in R80 and higher.

Description:
Legacy DHCP Relay services were found in the security rule base. Action is required in order for DHCP Relay to function properly post-upgrade.
Two possible options to solve the problem:
1). Remove legacy DHCP Relay services and add new DHCP Relay services. See sk104114 for instructions. This is the recommended action if managing only R77.20 gateways and above.
2). Keep legacy DHCP Relay services and make changes to the Gateways and the Security Management Servers. See sk98839 for instructions. Do this if managing any gateways which are older than R77.20.
Legacy DHCP Relay service(s):
bootp, dhcp-relay, dhcp-rep-localmodule, dhcp-req-localmodule

This document will be broken into 3 parts, the steps that must be done on the management side first and then two options, one for R77.10 and older gateways and one for R77.20-R77.30 gateways.

One warning on this process, you can only use one style of dhcp object per policy. So if you are using the new DHCP objects, the policy can only be used for R77.20 and newer gateways. If you need to use the legacy DHCP objects, the policy can only be used for R77.10 and lower gateways. Both DHCP object types (legacy and new) cannot be used together in the same policy.

Also, please note that this document assumes the management environment is an MDS (Multi-Domain Server) environment. This procedure should also work using a single SMS (Security Management Server), but please double-check the sk articles referenced in both Option A and Option B before proceeding.

Management Environment Required Patching:

1. Before any changes are made on the management side, it is recommended to update the R77.30 MDS environment (MDS & MLMs) to a minimum of R77.30 JHF Take 292 which can be downloaded via sk106162.

2. After the R77.30 management environment is on at least R77.30 Jumbo Hotfix Take 292, then the R77.30 Add-On package needs to be installed on the R77.30 MDS environment (all MDS & MLMs). The R77.30 Add-On package and instructions to install can be found in sk105412.

Option A – R77.20 and newer gateways using new DHCP objects (following sk104114)

R77.20 Security Gateway Required Patching:

1. R77.20 JHF Take 205 Needs To Be Applied
    a. JHF has to be obtained from Support
2. Hotfix for Issue ID 01613615 needs to be installed on top of R77.20 Take 205
    a. Hotfix has to be obtained from Support
3. Set the required value of kernel parameter *fwx_dhcp_relay_nat* - disable legacy NAT for DHCP Relay packets. (these steps are taken from sk116380)

Background:

Description	This parameter controls whether to apply legacy NAT to DHCP Relay packets: • "0" - does *not* apply legacy NAT to DHCP Relay packets • "1" - *apply* legacy NAT to DHCP Relay packets
Default value	• "1" in R77 GA / R77.10 / R77.20 / R77.30 • "0" in R80.10 and above

Notes	• This parameter is only used for ClusterXL / VSX cluster running DHCP Relay.
	• This parameter is *not available* for:
	  ○ Clusters not running DHCP Relay
	  ○ VRRP clusters
	  ○ Single Security Gateway

Procedure:

On ***each*** member of R77 GA / R77.10 / R77.20 / R77.30 cluster that runs DHCP Relay, set the value of kernel parameter *fwx_dhcp_relay_nat* to 0 (zero):

- To check the current value of this kernel parameter:

  [Expert@HostName]# fw ctl get int fwx_dhcp_relay_nat

- To set the value for this kernel parameter *on-the-fly* (does not survive reboot):

  [Expert@HostName]# fw ctl set int fwx_dhcp_relay_nat 0

- To set the desired value for this kernel parameter *permanently*:

  Follow sk26202 - Changing the kernel global parameters for Check Point Security Gateway.

  A. Create the *$FWDIR/boot/modules/fwkern.conf* file (if it does not already exit):

[Expert@HostName]# touch $FWDIR/boot/modules/fwkern.conf

B. Edit the *$FWDIR/boot/modules/fwkern.conf* file in Vi editor:

[Expert@HostName]# vi $FWDIR/boot/modules/fwkern.conf

C. Add the following line (spaces are not allowed):

fwx_dhcp_relay_nat=0

D. Save the changes and exit from Vi editor.
E. Check the contents of the *$FWDIR/boot/modules/fwkern.conf* file:

[Expert@HostName]# cat $FWDIR/boot/modules/fwkern.conf

F. Reboot the Security Gateway.
G. Verify that the new value was set:

[Expert@HostName]# fw ctl get int fwx_dhcp_relay_nat

4. Set the required size for the ARP cache table.

Background:

For installations with many DHCP clients, the default size of ARP table cache of 4096 entries may be insufficient.
If the ARP cache becomes full, an error message similar to the following will appear:

```
bootpgw_relay_reply: error installing hw 0:80:87:52:43:41 for
172.22.82.168 in ARP cache. error no = 105(No buffer space available)
```

Procedure:

If this occurs, follow these steps for Security Gateway / *each* cluster member:

a. Connect to command line.
b. Log in to Clish.
c. Increase the cache size from the default 4096 entries to 8192 entries:

HostName:0> set arp table cache-size 8192
HostName:0> save config
HostName:0> show arp table cache-size

R77.30 Security Gateway Required Patching:

5. R77.30 JHF Take 292 Needs To Be Applied
    a. JHF can be downloaded from sk106162.
6. Hotfix for Issue ID 01613615 needs to be installed on top of R77.30 Take 292
    a. Hotfix has to be obtained from Support
7. Set the required value of kernel parameter *fwx_dhcp_relay_nat* - disable legacy NAT for DHCP Relay packets. (these steps are taken from sk116380)

Background:

Description	This parameter controls whether to apply legacy NAT to DHCP Relay packets: • "0" - does *not* apply legacy NAT to DHCP Relay packets • "1" - *apply* legacy NAT to DHCP Relay packets
Default value	• "1" in R77 GA / R77.10 / R77.20 / R77.30 • "0" in R80.10 and above

Notes	• This parameter is only used for ClusterXL / VSX cluster running DHCP Relay.
	• This parameter is *not available* for:
	  ○ Clusters not running DHCP Relay
	  ○ VRRP clusters
	  ○ Single Security Gateway

Procedure:

On ***each*** member of R77 GA / R77.10 / R77.20 / R77.30 cluster that runs DHCP Relay, set the value of kernel parameter *fwx_dhcp_relay_nat* to 0 (zero):

- To check the current value of this kernel parameter:

  [Expert@HostName]# fw ctl get int fwx_dhcp_relay_nat

- To set the value for this kernel parameter *on-the-fly* (does not survive reboot):

  [Expert@HostName]# fw ctl set int fwx_dhcp_relay_nat 0

- To set the desired value for this kernel parameter *permanently*:

  Follow sk26202 - Changing the kernel global parameters for Check Point Security Gateway.

  A. Create the *$FWDIR/boot/modules/fwkern.conf* file (if it does not already exit):

     [Expert@HostName]# touch $FWDIR/boot/modules/fwkern.conf

  B. Edit the *$FWDIR/boot/modules/fwkern.conf* file in Vi editor:

[Expert@HostName]# vi $FWDIR/boot/modules/fwkern.conf

C. Add the following line (spaces are not allowed):

fwx_dhcp_relay_nat=0

D. Save the changes and exit from Vi editor.
E. Check the contents of the *$FWDIR/boot/modules/fwkern.conf* file:

[Expert@HostName]# cat $FWDIR/boot/modules/fwkern.conf

F. Reboot the Security Gateway.
G. Verify that the new value was set:

[Expert@HostName]# fw ctl get int fwx_dhcp_relay_nat

8. Set the required size for the ARP cache table.

Background:

For installations with many DHCP clients, the default size of ARP table cache of 4096 entries may be insufficient.
If the ARP cache becomes full, an error message similar to the following will appear:

```
bootpgw_relay_reply: error installing hw 0:80:87:52:43:41 for
172.22.82.168 in ARP cache. error no = 105(No buffer space available)
```

Procedure:

If this occurs, follow these steps for Security Gateway / *each* cluster member:

a. Connect to command line.
b. Log in to Clish.
c. Increase the cache size from the default 4096 entries to 8192 entries:

HostName:0> set arp table cache-size 8192
HostName:0> save config
HostName:0> show arp table cache-size

DHCP New Services Security Policy Updates for R77.20-R80.20:

1. Perform security policy changes documented in sk104114.
2. Since there are global properties being used, it would be recommended to only have R77.20 & up in domains that are using DHCP new services.

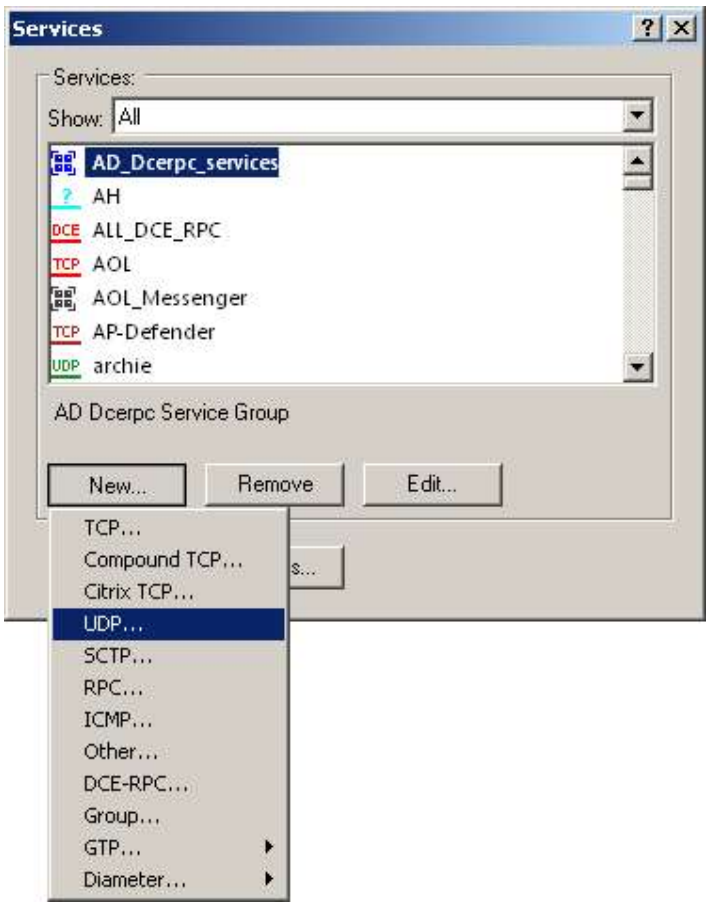
DHCP Relay Configuration At the Security Gateway Level for R77.20-R80.20:

1. Configure the DHCP relay configuration documented in sk104114.

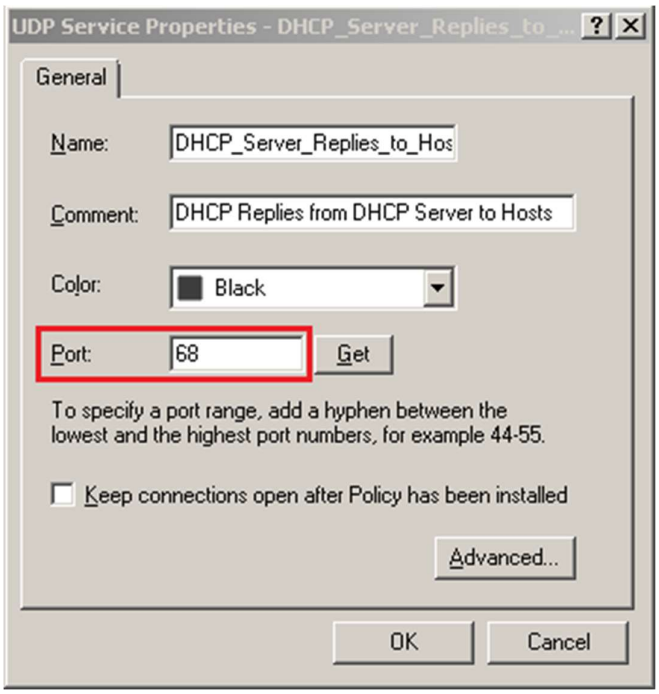
Option B – R77.10 and lower gateways using legacy DHCP objects (following sk98839)

Security Policy Changes Required For Domains that need to use legacy DHCP objects:

1. For domains that have gateways R77.10 and older, you will need to create a new UDP service for DHCP relay.
2. Once in the domain that contains the older gateways, go to the manage menu and click on services.
   a. 

3. Click on the new button and then select UDP
   a. 

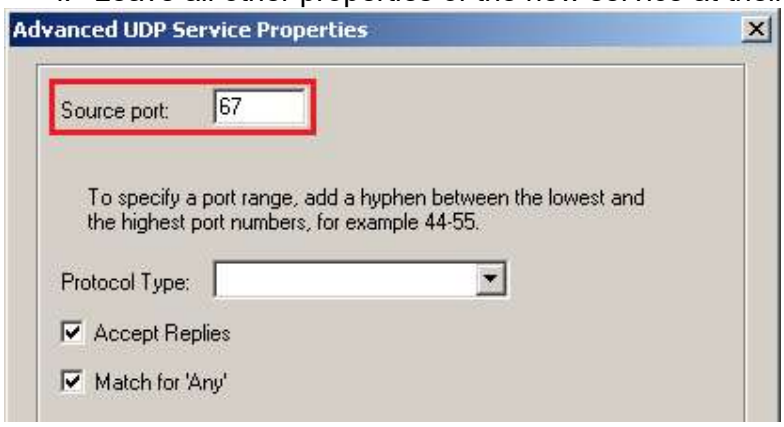
4. Create the new object.
   a. In the Name: field, enter the desired object name (e.g., DHCP_Server_Replies_to_Hosts).
   b. In the Comment: field, enter DHCP Replies from DHCP Server to Hosts.
   c. In the Port: field, enter 68.

d. 

e. Click on the Advanced button.

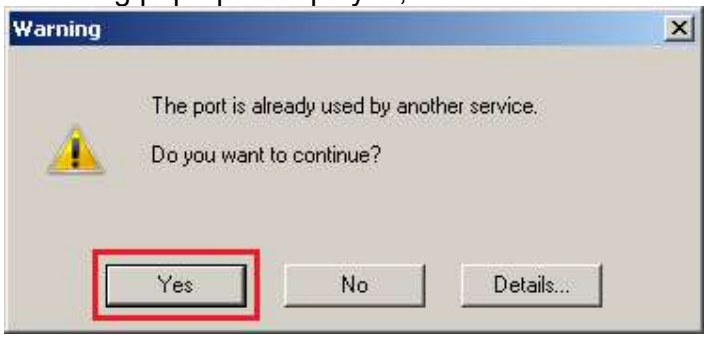
f. In the source port field enter 67

   i. Leave all other properties of the new service at their default

g. 

h. Click on the OK button

i. When a warning pop-up is displayed, click on "Yes" button:

   i. 

j. Click on "Close" button in the Services window.

k. Save the changes: Go to the File menu and click on Save.

5. Then follow the Security Policy configuration steps outlined in sk98839.

6. If there are NAT rules that match for DHCP traffic, you will also need to perform the NAT policy configuration that is documented in sk98839.

DHCP Relay Configuration At the Security Gateway Level for R77.10 and below:

1. Configure the DHCP relay configuration documented in sk98839.

